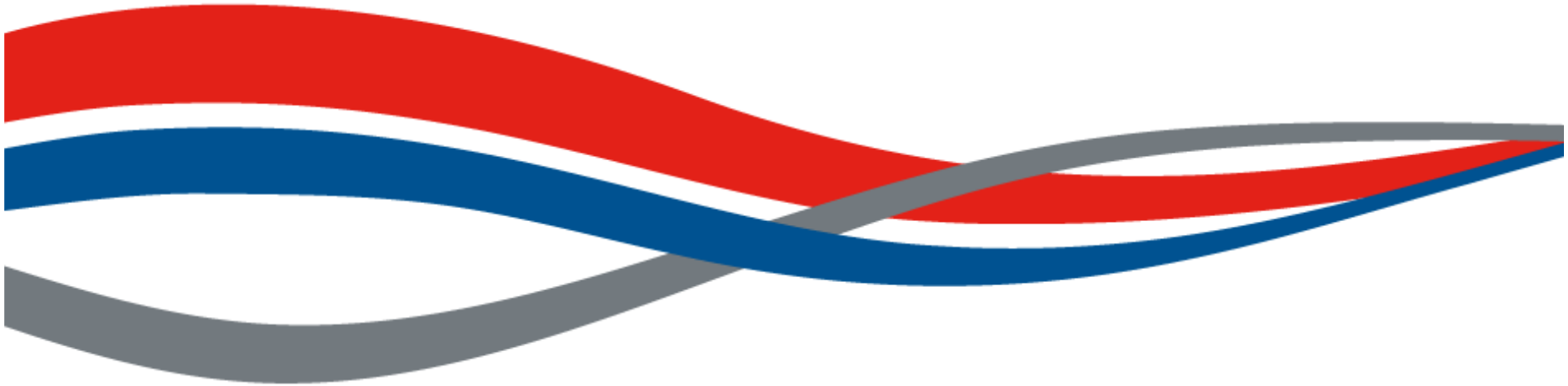
CP EXPO Workshop
«Risks and Security Management in Logistics and Transports»

Cyber Security in Railways Systems: Ansaldo STS experience

Part 1 – Cyber Security Issues in Customer Requirements

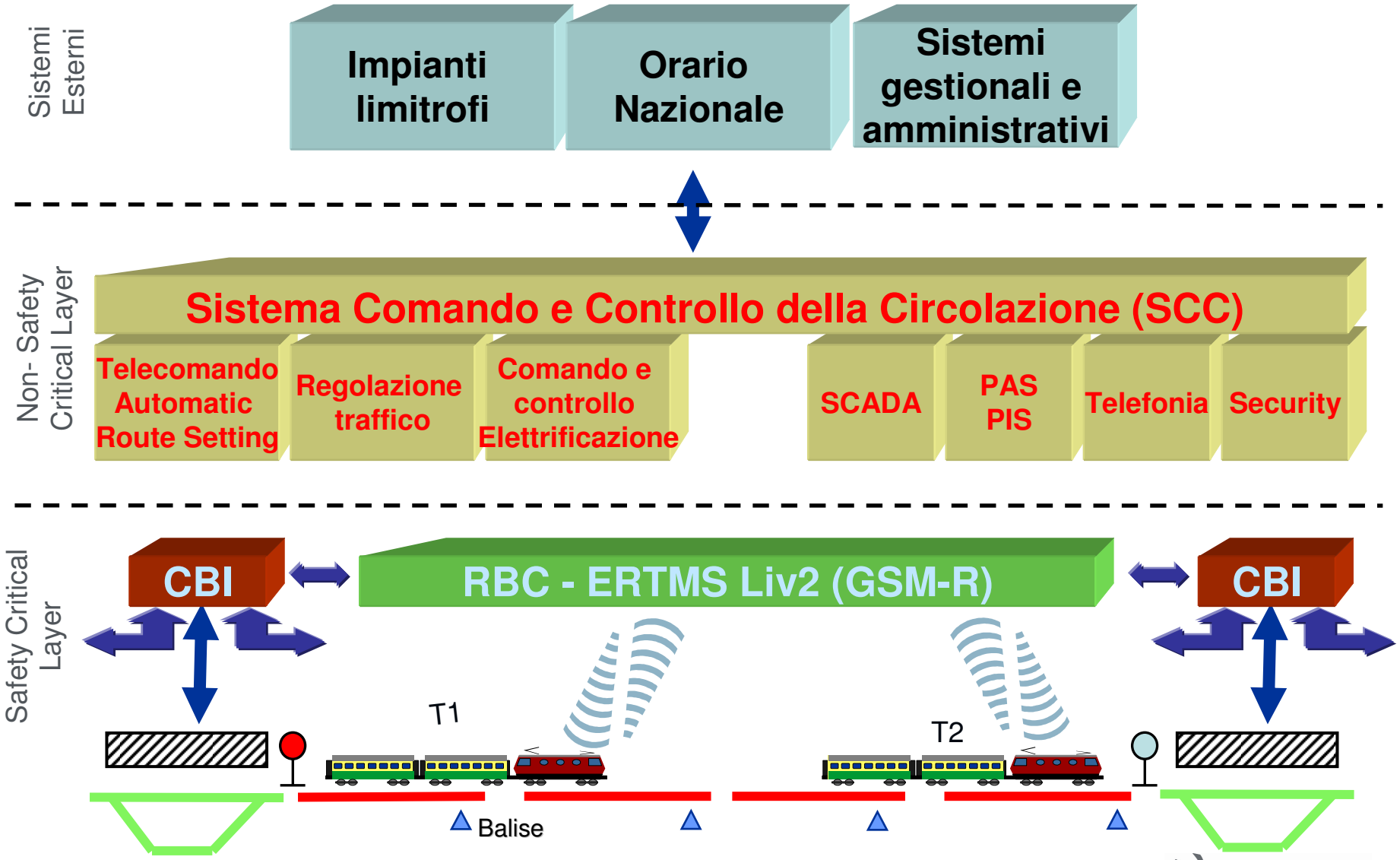


CP Expo Workshop

Genoa, October, 29th 2013

AnsaldoSTS
A Finmeccanica Company

L'impianto di segnalamento ferroviario



AnsaldoSTS
A Finmeccanica Company

Abstract

To be part of a bidding team is a good point of view to analyze how much the Customer's perception of the ICT security issues has changed during the last years.

The core functionalities required in a train automation system have not changed in the same period. However the adoption of ICT systems based on "open" paradigm and COTS components in the fields of computers and communication networks, induced new capabilities but also new security issues.

The first step of this path was the entrance, in the field of automation systems, of COTS hardware and, most of all, operating systems.

Even if these plants were still closed to external systems, they potentially suffered the effects of virus infections. The infected supports (FD etc) were the main entrance door. Even operators, more skilled with these operating systems than with the ones that were in use before, could become unintentional infection agents.

Hardening and antivirus were at that time the main ICT security counter measures, even if the same counter measures could induce a significant shift in systems complexity. For instance it has no meaning the installation of an antivirus system without any infrastructure for antivirus upgrade.

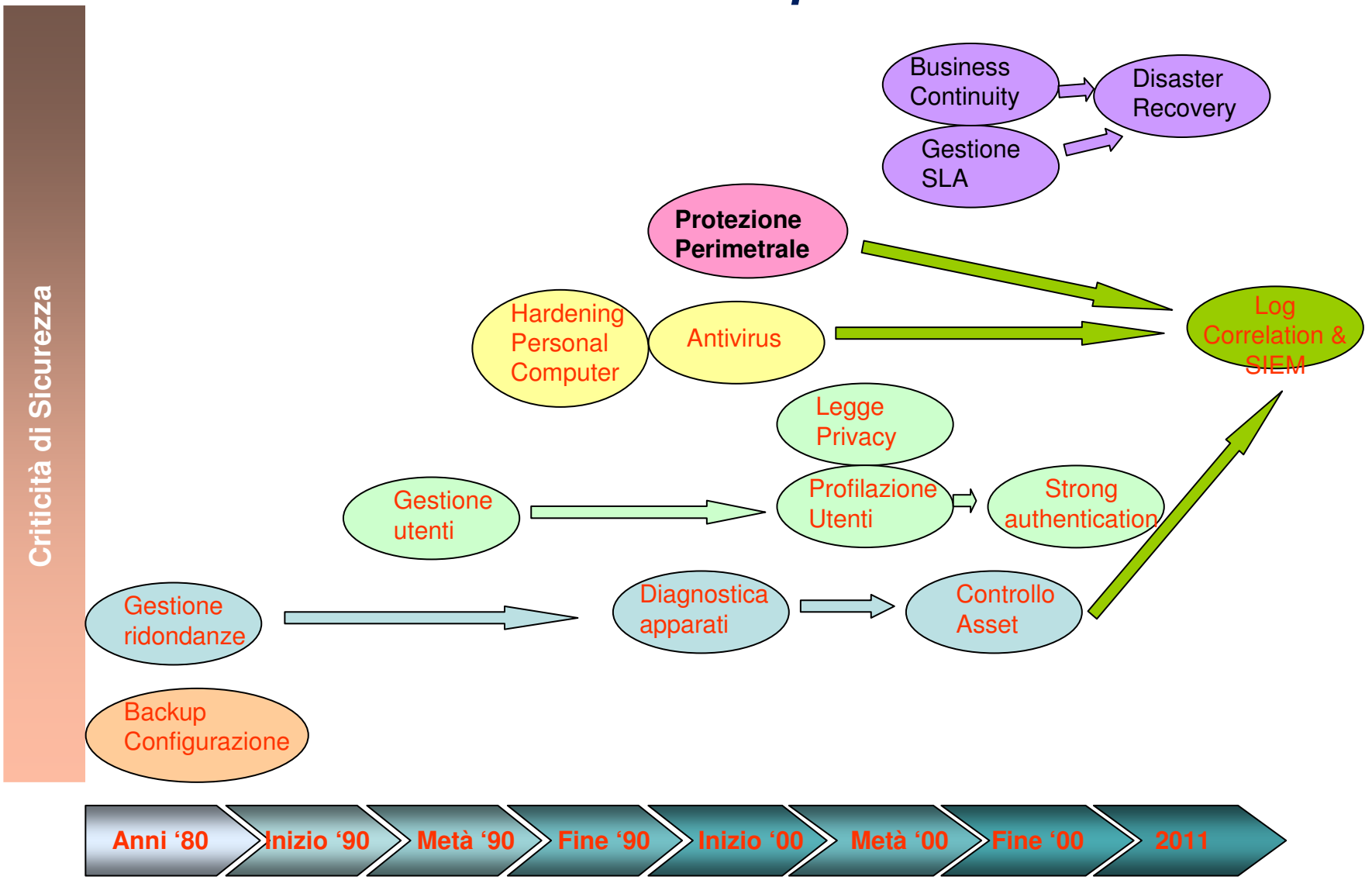
The introduction of geographic high speed data communication infrastructures allowed the development of regional sized supervision systems. These systems required integration between themselves and, moreover, with the national management systems at higher level. So a new security issue could arise relating to the communication with an external system potentially uncontrolled or requiring a different security level. The new two security counter measures are the formal definition for communication interfaces and perimeter protection.

Nowadays frontiers in railroad automation systems are relating to the system consolidation and mission critical data and application access by nomadic users (such as maintenance teams).

The related security items are: business continuity/disaster recovery, strong authentication, information security in fully virtualized systems.

From this short lookup arise the well know assumption that railroad world doesn't develop basic research, instead it deeply uses existing technologies that it adapts to its specific business needs. Compared with the past, however, the time spanning from the diffusion of a new ICT technology to its adoption in the railroad world is reduced asking for greater flexibility and faster integration.

Le Criticità di Sicurezza nella percezione del Cliente



AnsaldoSTS
A Finmeccanica Company